

Fireware XTM iOS/Android 対応 IPSec 設定手順



ウォッチガード・テクノロジー・ジャパン株式会社 2014 年 8 月 Rev-01

目次

はじめに	3
WatchGuard XTM 側の設定手順	4
モバイル機器側の設定手順	13
Android デバイス側の設定手順(Android Ver4.0.x & 4.1.x)	14
iOS デバイス側の設定手順(iOS Ver 4.x 以降)	19
おわりに	27

はじめに

本手順書は、Android Ver4.0.x & 4.1.x、iOS Ver4.x 以降 と Fireware XTM 11.7 をベースにした内容とな ります。また、WatchGuard XTM はファームウェア Fireware XTM 11.7(Build 番号:359571)以降のバー ジョンより対応しておりますので、事前にバージョン情報をご確認頂いてから実施ください。

WATCHGUARD XTM 側の設定手順

- 1. Policy Manager $\mathcal{O}[VPN] \Rightarrow [Mobile VPN] \Rightarrow [IPSec] 画面を開きます。$
- 2. "Mobile VPN with IPSec の構成"画面にて画面右上にある"追加"ボタンからウィザードを実行してください。

R Mobile VPN with IPSec の構成	x
±-OS	<u>}追加</u> 辆策 削除
To regenerate a set of mobile user configuration files, select a mobile	詳細
user group from the list above and click Generate. The Shrew Soft VPN client does not support all WatchGuard Mobile VPN with IPSec configuration settings. For a list of settings not supported by the Shrew Soft VPN client, click Help.	
この Firebox には、 Mobile VPN with IPSec ユーザーの機能キーが 405 人 す。 残りの数は 394 です。	分ありま
<u></u> K = キャンセル	ヘルフ

3. 下記が IPSec 構成設定の初期ウィザードの画面となります。そのまま"次へ"進みます。

Add Mobile VPN with IPSec	Wizard EX
N	ようこそ。
	Add Mobile VPN with IPSec Wizard 🔨
	このウィザードを使用して、モバイル ユーザー用の仮想プライベート ネットワークを作成することができ ます。
WatchGuard	詳細情報 <u>WatchGuard Mobile VPN with IPSec</u> 。 統行するには、[次へ]をクリックします。
	<戻る 次へ> キャンセル ヘルブ

4. 下記画面のように指定をします。尚、グループ名は iOS デバイスからの接続用とわかるような名前に することを推奨します。その後、"次へ"進めてください。

K Add Mobile VPN	with IPSec Wizard		×
ユーザー認証サ	ーバーを選択します。		WatchGuard
Firebox でモバイ)	レ <u>ューザーの認証に使用するサーバーおよびダ州</u> 「Einshaw DB	ブを選択します。	/
ある血(シーバー) グループ名:	iOS		\rightarrow
の グループ名	は認証サーバー上の有効なユーザー グループ名	を識別するために必要です。グ	ループ名では大文字と小文字が区別される
	してください。		
	<u>-//-</u> ,		
		<戻る 次へ >	キャンセル ヘルプ

5. 下記画面のように指定します。ここではシークレットキーを指定し、このシークレットキーは Android デバイスにも同じキーを設定する必要があります。ユーザーへ告知する必要があります。

Add Mobile VPN with IPSec Wiza	rd	
トンネル認証方法を選択します	0	WatchGuar
Firebox で安全な VPN トンネルを確	立するために使用する認証メソッドを選択します。	
😌 このパスフレーズを使用する	:	
トンネルのパスフレーズ:	•••••	
パスフレーズの再入力:	••••••	
◎ WatchGuard Management Se サーバーの管理用パスフレー IP アドレス:	rver が発行する RSA 証明書を使用します。 - ズを入力します。 	
管理用パスフレーズ:		
詳細情報 認証メソッド。		
	<戻る 次へ >	キャンセル ヘルプ

6. 下記画面のようにします。IPSec トンネルで許可したい接続先を指定出来ます。全てのトラフィックを XTM 経由とする場合は、"はい"を選択し"次へ"進めてください。

K Add Mobile VPN with IPSec Wizard	X
インターネット トラフィックのフローを指定します。	WatchGuard
モバイル コンピュータとインターネットとの間のすべてのトラフィックがトンネルを経由す	するようにしますか?
◎ いいえ、インターネット トラフィックをモバイル ユ・ザーの IBPに直接送信するよう	<u>うにします。(柔軟性は高く、安全性は低い)</u>
● はい、すべてのインターネット トラフィックがトンネルを経由するようにします。()	柔軟性は低く、安全性は高い
詳細情報 インターネット トラフィックがトンネルを経由するようにダイレクトします。	
(人)	++7210 (10)

7. 上記の手順にて全てのトラフィックを XTM 経由にした場合、下記の画面が表示されます。確認をして、"次へ"進んでください。

dd Mobile VPN with IPSec	Vizard	
・ンネル経由でアクセスできるリソースを特定します。		(W) atchGua
™トンネルを経由してモバイ	ル ユーザーがアクセスできるコンピュータおよびネットワーク	クを追加します。
種類 Alias	IPアトレス Anv-External	<u>35.00</u>
Network IP	0.0.0.0/0	HU KA:
8		

8. XTM へ IPSec 接続する際には iOS デバイスに仮想 IP アドレスを割り振ります。iOS デバイスへ割り 振る IP アドレスをホストアドレスまたはアドレス範囲から"追加"ボタンで登録してください。

K Add Mobile VPN with IPSec Wizard		×
仮想Pアドレスプールを作成します。		WatchGuard
Firebox でモバイル コンピュータに割り当てる IP アドレ	- スを追加します。	
10.0.1.200-10.0.1.220		<u>ìù hū</u>
🥠 この Firebox には、最大 405 人分の Mobile VPN v	with IPSec ユーザー ライセンスがあります。	
詳細情報 <u>仮想 IP アドレス</u> 。		
	(戻る) 次へ>	キャンセル ヘルプ

9. 下記がウィザード最終画面です。"完了"でウィザードを終了して下さい。尚、こちらで設定は終了で はありません。

K Add Mobile VPN with IPSec	Wizard		
N	Add Mobile VPN with IPSec Wizard が正常に完了しました。		
	おめでとうございます!モバイル ユーザー用の仮想プライベート ネットワークが新規作成されました。		
	The VPN configuration files are in the folder:		
	C:\Users\Public\Shared WatchGuard\muvpn\ 202.171.140.65\iOS\wgx		
	The .wgx file is encrypted with the tunnel passphrase.		
	The .vpn and .ini files are not encrypted. Use a secure method to distribute these files.		
	ウィザードが完了したら、チェックボックスを選択してユーザーをグループ "IOS" に追加してください。		
	── iOS にユーザーを追加する		
WatchGuard			
	<戻る キャンセル ヘルブ		

10. 再度手順 2 で実施した画面を開きます。Policy Manager の[VPN] ⇒ [Mobile VPN] ⇒ [IPSec]画 面を開きます。ウィザードで作成した構成(例では iOS)を選択して、"編集"画面を開いて下さい。

Mobile VPN with IPSec の構成	×
æ- <mark>ios</mark>	<u> </u>
	[]]][]]]][]]]][]]][]][]][]][]][]][]][]]
To regenerate a set of mobile user configuration files, selv user group from the list above and click Generate.	lect a mobile (生成
The Shrew Soft VPN client does not support all WatchGua with IPSec configuration settings. For a list of settings not he Shrew Soft VPN client, click Help.	ard Mobile VPN t supported by
この Firebox には、 Mobile VPN with IPSec ユーザーの機能 す。 残りの数は 394 です。	能キーが 405 人分ありま
<u>K</u> = + +	シセル ヘルプ

11. "全般"タブを選択します。ウィザードで設定済みの項目となるので、デフォルトで問題ありません。確認だけを行ってください。

般 IPsecトン	ネル「リソース」詳細
Firebox-DB -	
パスフレーズー	
このグループの 用します。)Mobile VPN with IPSec エンドユーザー フロファイルの暗号化に使
パスフレーズ	•••••
確認:	•••••
Firebox IP アド I	2
Mobile VPN with 1 つに接続しま	h IPSec クライアントはこれらの外部 IP アドレスまたはドメインの す。
	xxxx.xxxx.xxx.xxx
プライマリ:	
プライマリ: バックアップ:	
プライマリ: バックアップ: タイムアウトー	
プライマリ: バックアップ: タイムアウトー Firebox を認証 にタイムアウト	▼ サーバーとして使用する場合は、Firebox ユーザー アカウントごと *を設定します。
プライマリ: バックアップ: タイムアウトー Firebox を認証 にタイムアウト セッション:	▼ サーバーとして使用する場合は、Firebox ユーザー アカウントごと *を設定します。

12. "IPSec トンネル"タブを選択します。下記と同じように合わせてください。

「Mobile VPN with IPSec の構実」 グループ名: IOS	・トンネル認証メソッド
全般 IPsecトンネル リソース 詳細	エンドユーザプロファイルのパスフ・・・
トンネル認証メソッド ③ エンドユーザー フロファイルのパスフレーズを事前共有キーとして使用する	- ・フェーズ 1 設定
○ 証明書を使用 - フェーズ1設定	認証: SHA1
認証: SHA1 ▼ 暗号化: AES (256-bit) ▼	暗号化: AES(256bit)
-フェーズ2設定 フロボーザル PFS Diffie-Hellman Group1 マ	
	手順 13 へ進んでください。
	手順 14 へ進んでください。
<u>QK</u> キャンセル ヘルブ	

13. フェーズ1の詳細設定をします。下記のように合わせてください。

SA の有効期間:	1 hour	•	
キーグルーフ: 🔲	iffie-Hellman Group2	•	
VAT Traversal	キーブアライブ間	隔: 20	利
🖳 IKE キーブアライ	イブ メッセージ間	[蹑: 180 🛓	利
	最大失敗回	数: 3 🔹	-
V Dead Peer Detec	ction (RFC3706)		
	トラフィックのアイドル タイムアウ	ŀ: 90 ▲	利
	最大再試行回	数: 5 🚔	

※SA の有効期限は短めがセキュリティ上好ましいです。接続の安定性を望む場合はデフォルトの8時間にしてください。

14. フェーズ 2 のプロポーザル設定をします。下記のように合わせてください。

里菜: ESP (Encapsulating Security Payload)
認証:	SHA1
暗号化:	AES (256-bit)
	1 hour
	0 КВ

※キーの期限に関してはトラフィック容量単位ではなく時間単位にすることを推奨します。

15. "リソース"タブと"詳細"タブはウィザードにて設定済みの項目なので確認だけ行ってください。IPSecの構成設定は以上となります。

16. IPSec 用のアカウントを作成します。Policy Manager の[セットアップ] ⇒ [認証] ⇒[認証サーバ]画 面を開き、アカウントを下記のように作成して下さい。



- 17. 上記で作成した IPSec アカウントユーザに対して許可ポリシーを作成してください。
- 18. 再度 Policy Manager の[VPN] ⇒ [Mobile VPN] ⇒ [IPSec]画面を開きます。

19. 本手順にて作成した[グループ]を選択して[生成]をクリックします。

K Mobile VPN with IPSec の構成	×
• smartphone	<u> </u>
モバイル ユーザーの構成ファイルのセットを再作成するには、上記リス	詳細 生成
トでモバイル ユーザー グループを選択し、[作成] をクリックします。 Shrew Soft VPN クライアントは、 WatchGuard Mobile VPN with IPSec 0 すべての構成の設定をサポートしているわけではありません。 Shrew Soft VPN クライアントがサポートしていない設定のリストについては、 [ヘルプ] をクリックしてください。	,
この Firebox には、Mobile VPN with IPSec ユーザーの機能キーが 5 人分 残りの数は 0 です。 <u>Q</u> K キャンセル	あります。 ヘルプ

20. 下記のディレクトリに配布用のファイル(.wgm)が生成されます。

このファイル(.wgm)を各 Android 端末へ配布します。



モバイル機器側の設定手順

WatchGuard XTM 機器側の設定が完了したら、モバイル機器側の設定を行ないます。

Andonand デバイス、および iOS デバイスの設定方法について解説します。

Google Play で WatchGuard をキーワード検索します。
[WatchGuard Mobile VPN]が表示されますのでインストールします。





 あらかじめ Android へ配布されたファイル(.wgm)を端末に保存してください。 ファイルエクスプローラ可能なアプリで開き、クリックします。



3. 下記の画面が開きますので[XTM 設定手順]の項番 5 で設定したシークレットキーを入力します。次 に[Open]をクリックします。

Welcome
Please enter the password your administrator provided to open this file.
This application configures your VPN settings. Click on the icon in the lower right for more information. (j)

4. [View]をクリックします。

Welcome
Your device is ready. View the list of available connection profiles.
View
This application configures your VPN settings. Click on the icon in the lower right for more information.

5. プロファイルがインポートされ VPN 接続として表示されます。

表示されたプロファイルをクリックします。

VPN Connnection Prof	iles	
smartphone		

6. 接続メニューが表示されますので[Connect]をクリックします。



 リモート接続用に割り当てられた[Username]と[Password]を入力し、[Connect]をクリックします。
[Save Account Information]にチェックを入れると次回以降は アカウント情報が保存されます。

VPN Connnection Profiles		
smartphone		
IPSec VPN, Server Address		
Connect to smartphone		
Username		
watchguard		
Password		
••••••		
Save Account Infomation		
Connect Cancel		

8. [注意]画面が表示された場合は[このアプリケーションを信頼できるものとみなします。]にチェッ クを入れて、[OK]をクリックします。

mortabono ² <u>小</u> 注意		
WatchGuard Mobile VPNでVPN接続を作成しま す。		
続行すると、すべてのネット ワークトラフィックの傍受をア プリケーションに許可すること になります。信頼できるアプリ ケーションでない限り、同意し ないでください。誤って同意し た場合は、不正なソフトウェア によりデータが不正使用される 危険があります。		
このアプリケーションを □ 信頼できるものとみなし ます。		
キャンセル OK		

9. [Connected]と表示されれば接続完了です。



 App Store で WatchGuard をキーワード検索します。 インストールを実行します。



This application stores VPN profiles for use with WatchGuard XTM security solutions.

Contact your network administrator to get a profile for your network delivered by email.

No direct user interface functions are supported by this application.

1

2. あらかじめ iPhone/iPad へ配布されたファイル(.wgm)をクリックします。



3. [WatchGuard Mobile VPN で開く]をクリックします。



4. [XTM 設定手順]の項番 5 で設定したシークレットキーを入力します。 [Open]をクリックします。



5. 下記の画面が表示されますと完了です。[OK]をクリックします。



6. プロファイルが表示されますので[インストール]をクリックします。

キャンセル プロファイル		
A A A A A A A A A A A A A A A A A A A	smartphone WATCHGUARD	
- Junio	未署名 インストール	
説明	Profile description.	
受信日	2013/01/30	
内容	1個のVPN設定	
詳細	>	

7. [インストール]をクリックします。



8. 端末のセキュリティコードを入力します。

パス	コードを入力] キャンセル	
パスコードを入力			
1	2 АВС	3 Def	
4 сні	5 JKL	6 MNO	
7 PQRS	8 тих	9 wxyz	
	0	×	

9. リモート接続用に割り当てられたユーザー名を入力します。



10. 同様にリモート接続用に割り当てられたパスワードを入力します。



11. 下記画面が表示されたら完了です。



12. VPN プロファイルが登録されます。



13. [オン]にスライドし、VPN 接続を実行します。

設定	
🔂 機内モード	77
🛜 Wi-Fi	オフ >
VPN VPN	77
画 通知	>
🖌 位置情報サービス	オン >
⊾ キャリア	SoftBank >
動 サウンド	>
🐺 明るさ	>
쨅 壁紙	>

14. 正常に[オン]へスライドしますと、接続は完了です。

設定	
🏊 機内モード	77
🛜 Wi-Fi	オフ >
VPN VPN	オン
画 通知	>
🧹 位置情報サービス	オン 🔉
📞 キャリア	SoftBank >
動 サウンド	>
🐺 明るさ	>
🛒 壁紙	>

おわりに

iOS/Android 対応 IPSec 設定手順をご活用いただき、ありがとうございます。

このガイドを通して、ウォッチガード製品によっていかにモバイル機器による IPSec 接続が容易にできるか、 実感していただけたと思います。

WatchGuard XTM が御社のセキュリティ向上にお役に立てれば幸いです。